Breach – Find the Weakness

IT Planning Notes

Checking your fortifications!

Infinit Technology Solutions | www.infint-tech.com | 877-825-8340 (Toll Free)
7037 Fly Rd. | East Syracuse, NY 13057 | 315-432-1323 (Corporate Office)
201 Main Street | East Rochester, NY 14445 | 585-425-0668 (Rochester Office)

As part of developing your threat protection plan you need to find out what areas you might be lacking in that would leave you unprotected. Basically speaking, a "breach" is a gap in a wall, area, defense. It can exist because it was not found and remedied or it can be made by an attacker.

The following questions are more a thought process than a checklist. You want to start drawing a visual or graphic of your "fortifications" in order to find where there are gaps!

Process

How are plans, policies and procedures administered?

_____

Are you required to inform business partners of their responsibilities to meet specific security standards?

_____

Are there signed confidentiality agreements with all employees?

_____

Plan

Is there a written security plan for all areas of your operation?

_____

Is there a data recovery plan in case of a natural disaster? Has it been tested?

_____

Is there a plan that outlines how to deal with security incidents?

_____

Is there a plan in place to provide support for power management systems connected to your network devices?

_____

Policy

Are there policies that are appropriate to the customer information you handle?

_____

Is there a written security policy signed-off on by all employees outlining responsibilities and associated consequences for violations?

_____

Is there a procedure for adjusting passwords and other access points when employees leave?

_____

Procedure

Is there a procedure for verifying and authenticating user identity?

_____

Is there a procedure for shredding both paper and digital data before dumping?

_____

Are there testing procedures in place to test and look for known system vulnerabilities?

_____

Is there a procedure to ensure that intended data use is clearly defined and understood by all parties?

_____

Is there a procedure for regularly reviewing security processes, procedures, protocols and correcting any deficiencies?

_____

Access

Do you rank data by level of security when assigning access rights?

_____

Are background checks conducted on employees accessing medical, financial, or other forms of sensitive data?

_____

Have security needs including efforts to prevent and detect unauthorized use of information systems been defined? Is access monitored for unusual activity?

_____

Rank Yourself

Once you finish addressing all of these areas, rank yourself for each area of Process, Plan, Policy, Procedure and Access.

1 – I think we have this covered

2 - There may be a bit more work

3 – We are going to need to fix this

Once you have made some adjustments revisit these five areas and rank yourself again. Plan to revisit this on a quarterly basis so that you can keep your organization safe and secure!